CBA | CONSUMER BANKERS ASSOCIATION

April 12, 2021

Via Electronic Mail

Chief Counsel's Office
Attention: Comment Processing
Office of the Comptroller of the Currency
400 7th Street SW, Suite 3E–218
Washington, DC 20219

Ann E. Misback, Secretary
Board of Governors of the Federal Reserve System
20th Street and
Constitution Avenue NW
Washington, DC 20551

James P. Sheesley, Assistant
Executive Secretary
Attention: Comments
Federal Deposit Insurance Corporation
550 17th Street NW
Washington, DC 20429.

Re: Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers (Docket ID OCC–2020–0038 and RIN 1557–AF02; FRB Docket No. R–1736 and RIN 7100–AG06; FDIC RIN 3064–AF59)

Ladies and Gentlemen:

The Consumer Bankers Association ("CBA")[1] appreciates the opportunity to comment on the notice of proposed rulemaking[2] issued by the Office of the Comptroller of the Currency, the Board of the Federal

[1] The Consumer Bankers Association partners with the nation's leading retail banks to promote sound policy, prepare the next generation of bankers, and finance the dreams of consumers and small businesses. The nation's largest financial institutions, as well as many regional banks, are CBA corporate members, collectively holding two thirds of the industry's total assets.

[2] OCC, FRB, FDIC, Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers, Notice of Proposed Rulemaking and Request for Comment, 86 Fed. Reg. 2299 (Jan. 12, 2021).

Reserve System, and the Federal Deposit Insurance Corporation (collectively "the Agencies") relating to computer-security incident notification requirements for banks and their bank service providers.

Like most public and private entities, banks rely on interconnected computer systems to provide products and services to customers. In recent years, banks, as well as other institutions, have encountered numerous attempted cybersecurity attacks. With that being said, we support the Agencies' intention to ensure timely awareness of these incidents to promote the safety and soundness of the financial system.

CBA further supports the Agencies' desire to minimize the regulatory burden placed on banks to address significant cybersecurity incidents. However, CBA believes the proposed rule, as currently written, would trigger reporting of incidents below the intended threshold of critical cybersecurity incidents. Therefore, the proposed rule would lead to significant over-reporting, contrary to the Agencies' desired goal.

CBA submits the following suggestions to help ensure the Agencies' final rule achieves the appropriate amount of regulation. By reducing the regulatory burden, banks will be able to focus on protecting their customers in a crisis and restoring the integrity of their systems.

Clarify Definitions of "Computer-Security Incident" and "Notification Incident" to Right-size Regulatory Burden

Computer Security Incident

The definition of "computer-security incident" is overbroad and unclear as currently written. The proposed rule defines "computer-security incident" as "an occurrence which: (1) Results in actual or potential harm to the confidentiality, integrity, or availability of an information system or the information that the system processes, stores, or transmits; or (2) Constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies." This definition is overbroad for the purposes of the proposed rule and would result in a high volume of less significant or easily remediated occurrences, and the described incidents do not result in actual harm and should not rise to the level of a notification incident.

The first prong of this definition should limit occurrences to actual harm. "Potential harm" would include occurrences of no consequence to the proposed reporting framework. CBA also believes the first prong should be limited to information systems that give rise to a notification incident. For example, systems which carry out banking operations, activities, processes, or deliver banking products or services to external customers in the ordinary course of business. This additional clarification will help to ensure the Agencies' goal to ensure timely notification of any "significant computer-security incident that could jeopardize the viability of the operations of an individual banking organization, result in customers being able to access their deposit and other accounts, or impact the stability of the financial sector."

Notification Incident

The definition of "notification incident" is also overbroad and unclear as currently written. The proposed rule defines "notification incident" as "a computer-security incident that a banking organization believes in good faith could materially disrupt, degrade, or impair: (i) The ability of the banking organization to carry out banking operations, activities, or processes, or deliver banking products and services to a material portion of its customer base, in the ordinary course of business; (ii) Any business line of a banking organization, including associated operations, services, functions, and support, and would result in a material loss of revenue, profit, or franchise value; or (iii) Those operations of a banking

organization, including associated services, functions and support, as applicable, the failure or discontinuance of which would pose a threat to the financial stability of the United States."

CBA believes the current definition of notification incident would result in a significant compliance burden on banks with over-reporting of less significant or easily remediated events. Instead of including any computer-security incident that "could" materially disrupt, degrade, or impair the defined activities, CBA suggests replacing the word "could" in the "notification incident" definition with the phrase "is reasonable likely to." The current version would inadvertently include many less significant or easily remediated incidents. The modified definition would read as follows: "Notification incident" is an ". . .incident that a banking organization believes in good faith is reasonably likely to materially disrupt, degrade, or impair" the defined activities.

In conclusion, CBA urges the Agencies to provide more clear and precise definitions of "computer security incident" and "notification incident" to right-size regulatory burden on banks. As the Agencies have indicate, the purpose of this proposed rule is to standardize an informal practice. CBA would like banks during the time of crisis to have the bandwidth to remediate the issue.

Establish Procedures for Communicating with a Bank in Crisis

Change the 36-hour requirement

CBA urges the Agencies to review the proposed 36-hour requirement. We appreciate the good-faith nature of the rule as written. However, to allow additional flexibility during a time a crisis we would urge the Agencies to establish a time requirement between 48 and 72 hours.

Method of Notification

CBA recommends the Agencies provide notification may be satisfied by any of several methods, including, if applicable, notice to any member of the bank's on-site or supervisory team by any medium, to the regional office of the bank's primary regulator, or notice to an agency-designated point of contact.

During a time of crisis, some channels of communication may become inoperable or unsecure. In addition, a time of crisis could happen at any given moment, whether it is the start of a weekend, during a holiday, etc. A final rule allowing notification to any of several points of contact and through multiple channels would help to ensure timely notification and reduce burden and stress on banks as they seek to resolve the crisis event.

Notification Process

CBA urges the Agencies to provide banks with multiple options for providing notification. This will help ensure the Agencies receive timely notification during a cybersecurity incident.

Furthermore, regarding the content of the notification, we appreciate the Agencies' statement in the Preamble that the notification not include any specific information. However, given the importance of this issue to banks, CBA encourages the Agencies to incorporate this statement into the final rule.

Monitoring Procedure

In addition, a crisis event is extremely stressful on a bank. During an event when a notification incident has occurred, some bankers have expressed concerned about regulators wanting gratuitous updates during a crisis. CBA would encourage the Agencies to consider establishing a monitoring framework in the final

rule which would limit check-ins to every 48-hours during a crisis event. The purpose of the framework would be to minimize any interference with banks resolving the crisis event.

In general, CBA urges the Agencies to establish procedures during a crisis which would allow banks the flexibility to focus on the problem at hand to easily communicate with regulators. Banks understand the balance of keeping both the financial system secure and their customers secure. The Agencies should establish a framework of procedures that both respects and protects that understanding.

Describe How Agencies Will Handle Information

CBA would like for the Agencies to provide more clarity concerning how computer-security and notification incident information will be shared. We ask the Agencies to consider answering the following questions in the final rule: what happens to the information after banks provide notice to the regulators?; how are regulators allowed to follow-up on this information?; and how will regulators share this information with other regulators and other financial institutions?

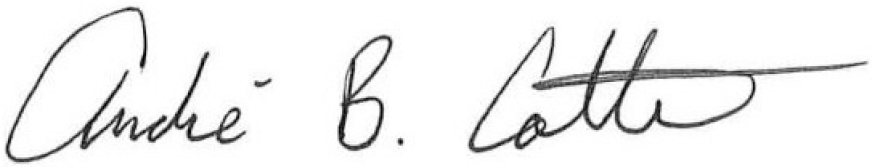
Ideally, CBA would not like any information shared to be attributed to a specific bank. We see the value in sharing this information with other agencies included in this NPR. However, we do not support other regulators or agencies having access to this information, unless it is anonymized.

Conclusion

With the rise of cybersecurity attacks, CBA agrees with the intent of this proposed rule to ensure the banking system is secure and prepared during a time of crisis. CBA further supports the Agencies' desire to minimize the regulatory burden placed on banks to address significant cybersecurity incidents. However, CBA believes the proposed rule, as currently written, would trigger reporting of incidents below the intended threshold of critical cybersecurity incidents. CBA encourages the Agencies to consider the comments provided and to develop a final rule that appropriately tailors regulation to the desired outcome.

If you have any additional questions or concerns, please do not hesitate to contact André Cotten at 202-552-6360 or at Acotten@consumerbankers.com.

Sincerely,



André B. Cotten, Esq.
Assistant Vice President, Regulatory Counsel
Consumer Bankers Association